



U.S. FISH AND WILDLIFE SERVICE TRANSMITTAL SHEET

| | | |
|--|------------------------|--------------------------------|
| PART | SUBJECT | RELEASE NO. |
| 270 FW 1, 2, 4, 6, 7 & 8 | ITM Program Management | 406 |
| FOR FURTHER INFORMATION CONTACT Division of Information Technology Management | | DATE September 30, 2002 |

EXPLANATION OF MATERIAL TRANSMITTED:

270 FW 1 describes the Fish and Wildlife Service Information Technology Architecture (SITA).

270 FW 2 defines policies for planning and managing investments in information technology and automated information systems.

270 FW 4 establishes policies and procedures for performing management control reviews of automated information systems in the Service.

270 FW 6 defines data management practices and the process for establishing data standards.

270 FW 7 identifies the policies, procedures, and responsibilities that form the basis of the Service's automated information technology (IT) security program.

270 FW 8 states the objectives of the spatial data management program.


Deputy DIRECTOR

FILING INSTRUCTIONS:

Remove:

270 FW 3, 03/08/94, FWM 130 (5 pages)
270 FW 4, 03/08/94, FWM 130 (4 pages)
Illustration 1, 270 FW 4, 03/08/94, FWM 130 (1 page)
Illustration 2, 270 FW 4, 03/08/94, FWM 130 (1 page)
270 FW 7, 10/13/92, FWM 042 (4 pages)
Exhibit 1, 270 FW 7, 10/13/92, FWM 042 (2 pages)
Appendix 1, 270 FW 7, 10/13/92, FWM 042 (3 pages)
Appendix 2, 270 FW 7, 10/13/92, FWM 042 (1 page)
Appendix 3, 270 FW 7, 10/13/92, FWM 042 (2 pages)

Insert:

270 FW 1, 09/30/02, FWM 406 (2 pages)
270 FW 2, 09/30/02, FWM 406 (5 pages)
270 FW 4, 09/30/02, FWM 406 (4 pages)
270 FW 6, 09/30/02, FWM 406 (3 pages)
270 FW 7, 09/30/02, FWM 406 (6 pages)
Exhibit 1, 270 FW 7, 09/30/02, FWM 406 (4 pages)
Exhibit 2, 270 FW 7, 09/30/02, FWM 406 (2 pages)
Exhibit 3, 270 FW 7, 09/30/02, FWM 406 (2 pages)
Exhibit 4, 270 FW 7, 09/30/02, FWM 406 (4 pages)
270 FW 8, 09/30/02, FWM 406 (3 pages)

**FISH AND WILDLIFE SERVICE
INFORMATION RESOURCES MANAGEMENT**

Information Resources Management

Part 270 ITM Program Management

Chapter 4 Management Control Reviews of Automated Information Systems

270 FW 4

4.1 What is the purpose of this chapter? This chapter establishes policies and procedures for performing Management Control Reviews (MCR) of automated information systems in the Service. These reviews are part of an overall risk management strategy and will determine if systems are operating within an acceptable level of risk. The review process addresses management controls, practices and policies as well as associated technical issues. Regular reviews will result in the early identification of potential problems and permit more cost-effective remedies. A properly oriented review program will also identify beneficial policies, practices, and products that could be adapted and shared by other users within the Service.

4.2 Why are MCRs required for automated information systems? Various Federal laws and policies mandate a 3-year review cycle for automated information systems.

A. 375 DM 5, IRM Program Review.

B. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources.

C. OMB Circular A-127, Financial Management Systems.

D. 340 DM, Management Accountability and Control.

E. Federal Managers' Financial Integrity Act of 1982.

F. 290 FW 1-3, Management Control Systems.

4.3 How does this chapter relate to other Service policies? Chapter 270 FW 2 deals with the general requirements for initiating and funding a system to become part of the Service's Information Technology (IT) investment portfolio and for managing its life cycle. This chapter articulates the requirements to integrate periodic reviews into the life cycle. 270 FW 1 states policy on IT architecture with which Service systems must conform. 270 FW 7 focuses on specific IT security requirements that are a critical part of a system's life cycle.

4.4 What is the Service's MCR policy for automated information systems?

A. Every automated information system that is classified as either a major application or a general support system (GSS) will be part of the Service's MCR schedule.

B. Each major application will have an MCR in the form of an independent audit of its security controls at least every 3 years.

C. Each GSS will have an MCR in the form of an independent audit or a self review of its security controls at least every 3 years.

D. A major application or GSS not scheduled for an MCR should have its accreditation documentation reviewed annually to ensure that it is current. See 270 FW 2.

E. Service implementation of Departmental Administrative Systems or other Departmentally mandated automated information systems will be considered to be major applications and subject to MCRs.

4.5 What are the major components of MCRs of automated information systems? Reviews should adhere to the following methodology, whether independent reviews or self reviews.

A. Form an MCR team. The system owner should appoint a team and a team leader to conduct the MCR. If the MCR is a self review, the team leader and most team members will be from the Program or Region whose system is being reviewed, but it should contain at least one member from a different Program or Region. If the MCR is an independent audit, the team leader and members will be from other Programs and Regions, or will be contractors, but the team should contain at least one member from the Program or Region whose system is being reviewed. The team conducts the onsite reviews and collects the review data.

B. Brief the system owner. The team leader should present a briefing to the system owner to identify review objectives and a schedule of activities, discuss the methodology, evaluate the checklists and questions, and to recommend additions or modifications. The team leader will also discuss any specific areas of concern that the local managers want addressed.

C. Review the system's controls. Those responsible for conducting an MCR should use FWS Form 3-2232 (MCR Checklist for Automated Information Systems). For each control on the checklist, review the controls that are in place, determine if they are effective, and identify possible vulnerabilities. Review all documentation relevant to each item. Interview the system owners, the system manager, the system security manager, and selected users to verify answers. Conduct appropriate tests of system operations. Document the methodology and the results obtained. The reviews should be accomplished in the most efficient manner for the Region or Program using telephone interviews where appropriate. Summarize results on the checklist.

D. Identify control weaknesses. The team should analyze the findings from the checklist and summarize them on FWS Form 3-2234 (General Controls Profile) for each category of control. Indicate if the overall control is in place and effective, and whether or not there is an alternative. Evaluate the potential for control weakness as high, medium, or low. See the instructions for this form for more information on identifying non-material or material control weaknesses. The team should also review the

**FISH AND WILDLIFE SERVICE
INFORMATION RESOURCES MANAGEMENT**

Information Resources Management

Part 270 ITM Program Management

Chapter 4 Management Control Reviews of Automated Information Systems

270 FW 4

findings of previous audits and reviews to ensure that corrective actions have been addressed.

E. Evaluation of results by system owner. The team leader should brief the system owner on the results and discuss possible corrective actions.

F. Identify Corrective Actions. For each reportable control weakness on FWS Form 3-2234, determine corrective actions and completion dates, and report them on FWS Form 3-2233 (Control Evaluation Report). Obtain input from persons responsible for completing corrective actions before the corrective actions are final.

G. Complete the Automated Information System Accreditation. See FWS Form 3-2231.

H. Report the results of the MCR. Submit the completed checklist, General Controls Profile, and if applicable, the Control Evaluation Report with a cover memorandum containing the information about the review to the Chief, Division of Policy and Directives Management (Attention: Service Management Control Coordinator) with copies to ITM-WO before July. The cover memorandum must contain the following information:

(1) A general description of the system, including name, location, description of hardware and software, number of users, type of information processed, and other pertinent information.

(2) A statement to the effect that either:

(a) "All prescribed controls or alternate controls are in place and effective, as indicated in the General Controls Profile, and no known control weaknesses in the system exist." or

(b) "The lack of prescribed controls or alternate controls or the failure of these controls to be effective, as indicated in the General Controls Profile, has resulted in the control weaknesses identified in the Control Evaluation Report."

(3) A list of the functional elements and controls that were excluded from the evaluation and the reasons they were excluded.

(4) A list of any alternative functional elements or controls, and the controls they replaced.

(5) A brief summary of the tests that were conducted to validate the functional elements; which functional elements received special in-depth testing; and the reason for the special tests.

(6) The organizational component(s) that conducted the control evaluation.

4.6. What are the procedures for conducting Information Technology MCRs? The team members will have an orientation session prior to the start of the review process to present standards for appropriate and ethical behavior during the review will be presented. These include:

A. Team members will be advised to look for and identify positive factors as well as non-compliance items so that the information presented to management will provide a balanced and complete representation of the environment under review.

B. Team members will be advised to follow as closely as possible the interview questions and checklists provided. Gathering of collateral information is encouraged, but branching off into new topic areas without prior notice to the system owner and approval of the team leader should be avoided.

C. During the review process, team members will refrain from conducting business not directly related to the review. Team members will not file any independent reports relative to review findings and corrective actions.

D. Points of contact for the reviews and interviews will be obtained, times identified, and a schedule of activities developed. Every effort will be made to minimize disruption and impact on the resident workforce.

E. Review assignments will be given and set times for meeting to discuss, record, and consolidate findings will be established.

F. On the last day of the review, a meeting will be set for the team to brief the system owner. The findings and corrective actions developed will be presented and discussed. The findings will include both positive and negative items. The team leader will provide a signed copy of findings to the system owner.

4.7 How will corrective actions be tracked? Corrective actions will be tracked by the Service. The Department tracks the correction of material weaknesses. After completion of a corrective action, the system owner will fill out and submit FWS Form 3-2147 (Certification of Completed Corrective Action) to the Service Management Control Coordinator.

4.8 Who is responsible for implementing the provisions of this chapter?

A. The Director provides the high-level visibility and support required to implement and maintain a viable and effective Information Technology Management Control Review Program.

B. Assistant Directors and Regional Directors are responsible for:

**FISH AND WILDLIFE SERVICE
INFORMATION RESOURCES MANAGEMENT**

Information Resources Management

Part 270 ITM Program Management

Chapter 4 Management Control Reviews of Automated Information Systems

270 FW 4

(1) Implementing the Service's Management Control Review Program within their Program or Region in accordance with this chapter.

(2) Funding independent reviews or self-reviews for major applications as appropriate.

(3) Funding independent or self reviews for GSS as appropriate.

(4) Reviewing all findings and corrective actions resulting from MCRs of automated information systems and taking action to address pertinent issues.

C Automated Information System Owners are responsible for:

(1) Reporting new major applications and GSS to ITM-WO. This should be part of the process described in 270 FW 2.

(2) Preparing funding requests for independent reviews or self-reviews of major applications every 3 years.

(3) Preparing funding requests for independent or self-reviews of GSS every 3 years.

(4) Implementing corrective actions identified in MCRs in a timely manner.

(5) Annually reviewing system accreditation documentation for major applications and GSS per 270 FW 2.

D. Chief, ITM-WO is responsible for:

(1) Identifying major applications and GSS as part of the Service's IT portfolio. See 270 FW 2.

(2) Managing a 3-year review cycle for major applications and GSS.

(3) Reviewing MCR reports and providing PDM with comments and recommendations.

E. The Service Management Control Coordinator is responsible for:

(1) Providing ITM-WO copies of MCR reports for review and comments as necessary.

(2) As assigned, transmitting MCR reports from the Service to the Department.

F. MCR Team Leaders are responsible for:

(1) Coordinating with the system owners to establish a satisfactory review schedule.

(2) Determining control tests and identifying personnel to be interviewed and topics of interviews.

(3) Determining local support requirements, such as personnel, equipment, office space, etc.

(4) Coordinating with system owners to select MCR Teams.

(5) Developing schedule for briefing system owners at the outset and the conclusion of MCRs.

(6) Preparing reports of findings and planned corrective actions.

(7) Preparing any required Departmental and Service reports or products.

4.9 What special terms do I need to know?

A. Automated Information System. A discrete set of information and IT organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Automated Information systems include both general support systems and major applications as those terms are defined in OMB Circular A-130, Appendix III. Examples are local and wide area networks, telecommunications systems, electronic mail systems, geographic information system (GIS) projects, data creation projects, databases, and radio projects.

B. General Support System (GSS). A term from OMB Circular A-130, Appendix III, meaning an interconnected set of information resources under the same direct management control which shares common functionality and normally includes hardware, software, information, data, applications, communications, and people. Examples are local and wide area networks, telecommunications systems, and electronic mail systems.

C. Automated information system owner. The manager who makes the decision to fund the automated information system and who is responsible for the development, acquisition, operation and maintenance of the system.

D. Independent review. A review that is conducted by a group outside of the program or Region whose system is being reviewed.

E. Major Application. A term from OMB Circular A-130, Appendix III, which means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Do not confuse this use of "major" with its use in the term "major automated information system" in 270 FW 2, OMB Circular A-11, and the body of A-130, where it designates certain levels of capital investment for a system.

**FISH AND WILDLIFE SERVICE
INFORMATION RESOURCES MANAGEMENT**

Information Resources Management

Part 270 ITM Program Management

Chapter 4 Management Control Reviews of Automated Information Systems

270 FW 4

F. Management Controls. The organization, policies, and procedures used by agencies to reasonably ensure that: programs achieve their intended results; resources are used consistent with agency mission; programs and resources are protected from waste, fraud, and mismanagement; laws and regulations are followed; and reliable and timely information is obtained, maintained, reported, and used for decision making.

G. Material Weakness. A serious deficiency that is reported up through management levels to the Department. The Management Control and Audit Follow-Up Council determines whether or not a weakness is material, and should be reported outside the Department. See 290 FW 1.

H. Self-Review. A review conducted by the program or Region whose system is being reviewed.